UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/700,656	02/14/2001	Harald Vater	JEK/VATER	7577

7590 07/19/2007

Bacon & Thomas
Fourth Floor
625 Slaters Lane
Alexandria, VA 22314-1176

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
07/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/700,656	VATER ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 November 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) *1-25,34-41 and 43* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *26-33 and 42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A reply to the Final Office action under 37 CFR 1.116 was received on 11 October 2006. By this reply, Claims 33 and 42 were amended. No claims were added or canceled. Although the reply did not fully comply with the requirements of 37 CFR 1.121, the amendment was nevertheless entered, as indicated in the Advisory action mailed 26 October 2006. A supplemental after-Final reply, which corrected the issues of non-compliance with 37 CFR 1.121, was received on 20 November 2006, concurrently with a Notice of Appeal and a Pre-Appeal Brief Request for Review. An initial Notice of Panel Decision was mailed on 04 December 2006, and a supplemental Pre-Appeal Brief Request for Review was received in response on 20 December 2006. A further Notice of Panel Decision was mailed on 04 May 2007.

2. Claims 1-43 are currently pending in the present application. Claims 1-25, 34-41, and 43 were previously withdrawn from further consideration as being directed to nonelected inventions. Claims 26-33 and 42 are currently under consideration in the present application.

Response to Arguments

3. As noted in the Notice of Panel Decision from Pre-Appeal Brief Review mailed 04 May 2007, in view of the Pre-Appeal Brief Request for Review filed on 20 November

2006, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

Claim Rejections - 35 USC § 112

4. As noted in the Advisory action mailed 26 October 2006, the rejection of Claim 42 under 35 U.S.C. 112, second paragraph, as indefinite, is withdrawn in light of the amendments to the claims.

Claim Rejections - 35 USC § 102

5. Claims 26-33 and 42 are rejected under 35 U.S.C. 102(e) as being anticipated by Kocher et al, US Patent Application Publication 2002/0124178.

In reference to Claim 26, Kocher discloses a method of protecting secret data, where the method includes falsifying input data by combination with auxiliary data before execution of one or more operations (paragraphs 0068, 0070, and 0072, where blinding occurs before permutation operations), and combining the output data with an auxiliary function value in order to compensate for the falsification of the input data (paragraphs paragraphs 0070, 0072, and 0073, where unblinding occurs to compensate for the blinding), where the auxiliary value was previously determined by executing the operations using the auxiliary data as input data in safe surroundings (paragraph 0072, where the output buffer is initialized with the blinding bit and the data in the output buffer is the result of using the input permutation table, i.e. the operations).

In reference to Claim 27, Kocher further discloses that the combination with the auxiliary function value is performed before execution of a non-linear operation (see paragraph 0074, where inputs can be maintained in a blinded state and only reconstituted when nonlinear operations must be performed).

In reference to Claim 28, Kocher further discloses that the auxiliary data are varied (paragraphs 0072-0075).

In reference to Claims 29-32, Kocher further discloses that new auxiliary values can be generated by combining existing values, that auxiliary data are selected

randomly, pairs of auxiliary data and auxiliary function values are generated, and the auxiliary data are random numbers (see paragraphs 0072 and 0075).

In reference to Claim 33, Kocher further discloses combining the output data and auxiliary function value using an XOR operation (see paragraph 0073).

In reference to Claim 42, Kocher further discloses that operations include permutations of data (see paragraphs 0068 and 0070-0074).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Wood, US Patent 5003596, discloses a cryptographic system that uses permutations and mask values in encryption.

b. Wood, WIPO Publication WO91/03113, is an international application publication corresponding to US Patent 5003596.

c. Delaporte et al, US Patent 5168521, discloses an encryption system in which permutations are performed and a masking system is used.

d. Ohki et al, US Patents 6615354 and 6631471, disclose systems for use in smart cards in which input data is transformed using disturbance data before performing processing and processed disturbance data is combined with the processed data to compensate for the original transformation. It is noted that

these references do not constitute prior art to the present application, but are included for the sake of completeness.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ZAD
zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER